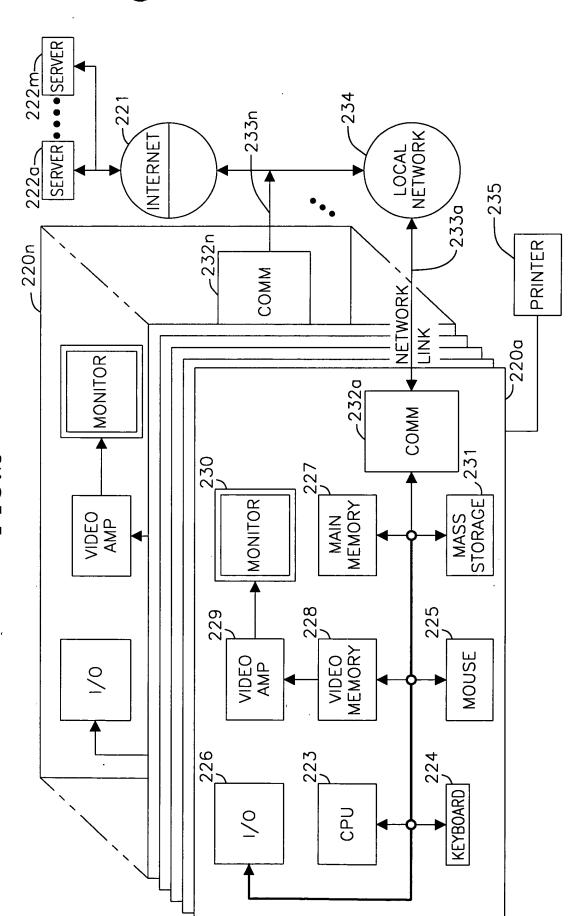


The state of the s

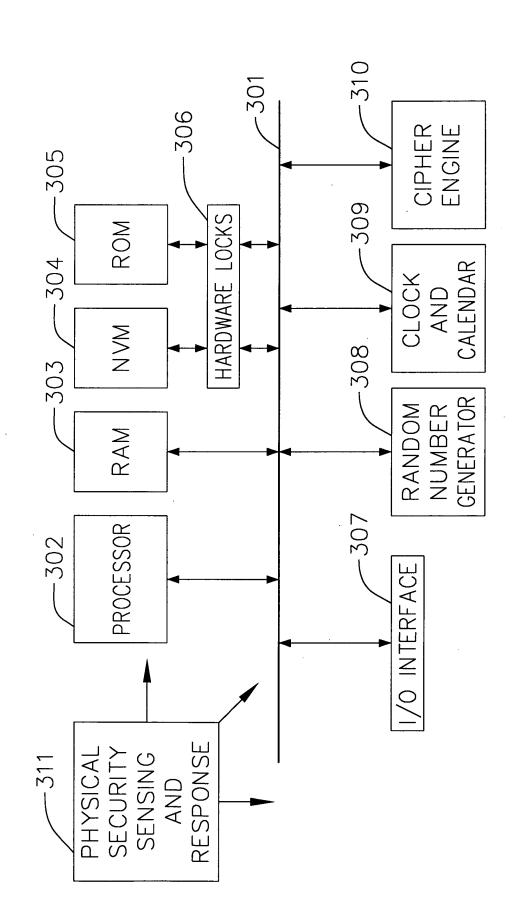
FIG.2

Control of the contro



APPROVED	O.G. FIG.	
BY	CLASS	SUBCLASS
DRAFTSMAN		

FIG.3



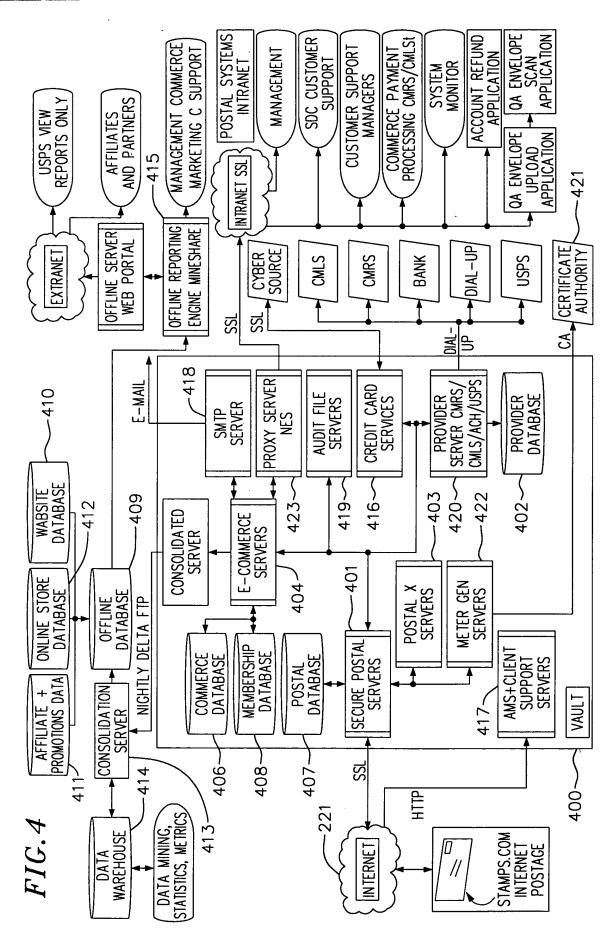
ijĢ

2 3

Ì:≟

15

[,≟



O.G. FIG APPROVED CLASS SUBCLASS DRAFTSMAI

FIG.5

GENERATES A RANDOM, 64-BIT CHALLENGE CLIENT SOFTWARE

CLIENT SOFTWARE

THE CHALLENGE IT SENT WITH • COMPARES THE HMAC OF THE HIMAC IT RECEIVES FROM THE PSD.

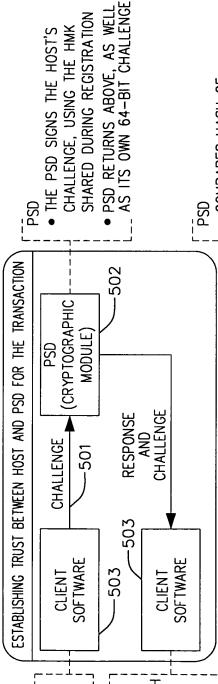
HOST TRUSTS THE PSD FOR THIS TRANSACTION.

CHALLENGE TO AUTHENTICATE HOST RETAINS PSD'S TSELF TO THE PSD

CUSTOMER'S ASCENDING AND SIGNS CHALLENGE THAT THE PSD SENT, AND ALSO THE **-OCAL RECORD OF THE** DESCENDING REGISTERS. SENDS THIS TO PSD. CLIENT SOFTWARE

SENDS CLEARTEXT OF THE RANSACTION MESSAGE. CHALLENGE AND THE

SENDS AN HMAC OF ALL OF THE ABOVE, USING SHARED



SHARED DURING REGISTRATION

CHALLENGE, USING THE HMK THE PSD SIGNS THE HOST'S

CALCULATION OF THE SAME WAS NOT TAMPERED WITH. THIS ENSURES MESSAGE RESPONSE WITH LOCAL COMPARES HASH OF

ESTABLISHING TRUST BETWEEN PSD AND HOST FOR THE TRANSACTION

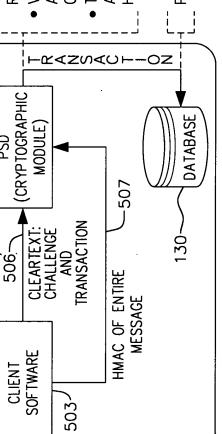
-502

SIGNED CHALLENGE TO AND AR/DR

505-

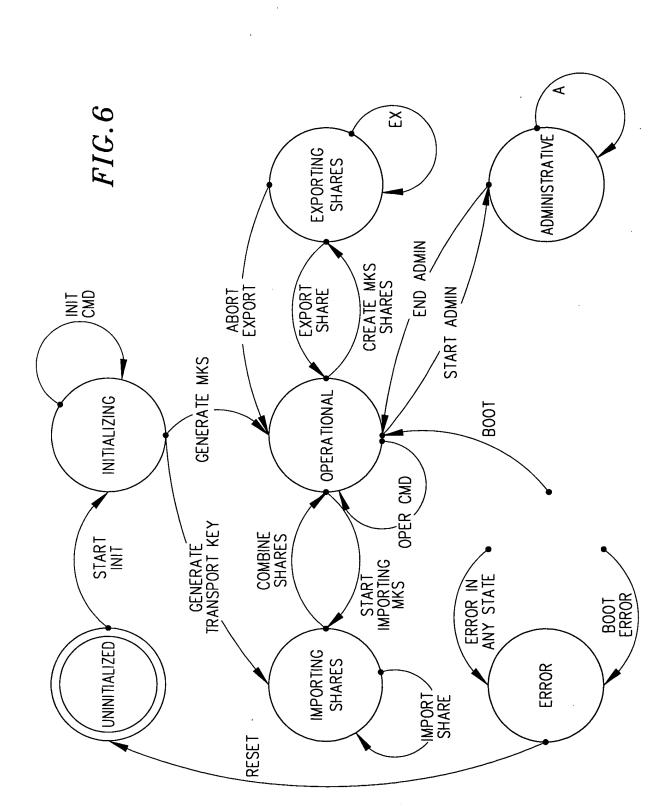
RECEIVED IS CHALLENGE SENT. VERIFIES HOST'S REGISTERS ARE SAME AS LOCAL DATA VERIFIES CHALLENGE OF REGISTERS.

THIS ABOVE TWO STEPS **AUTHENTICATE THE** PSD PERFORMS TRANSACTION



HT I'T SEE THE SEE SEE SEE

13



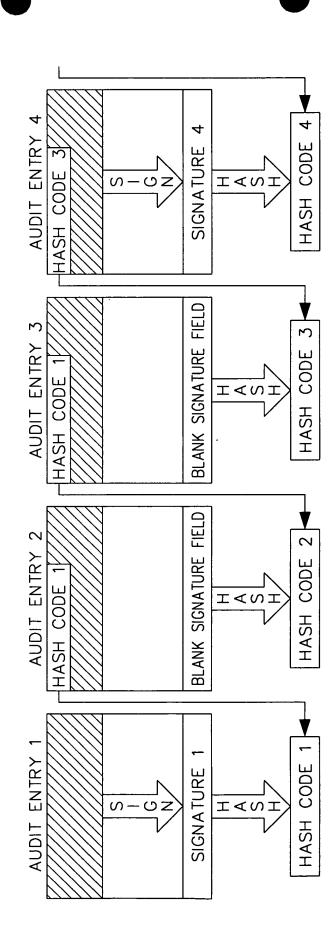
APPROVED O.G. FIG.

BY

CLASS SUBCLASS

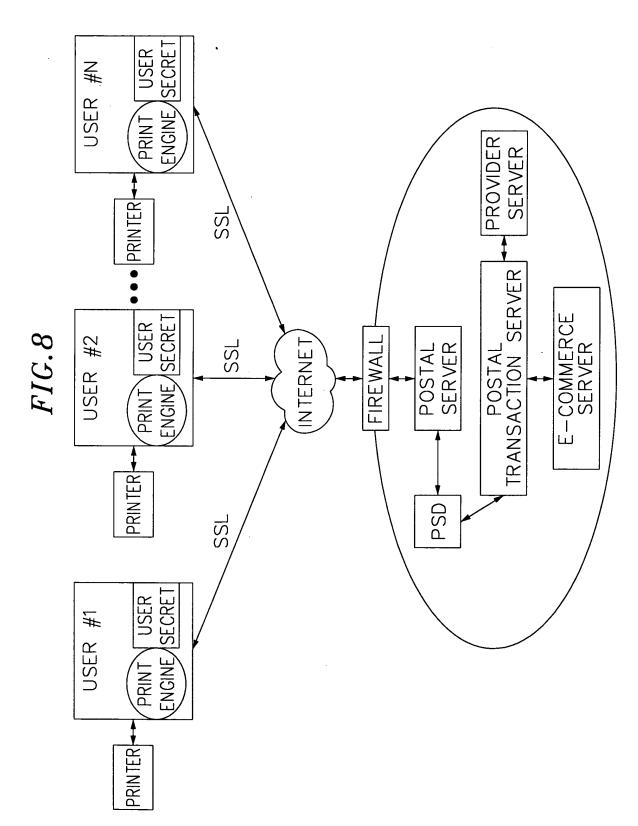
DRAFTSMAN

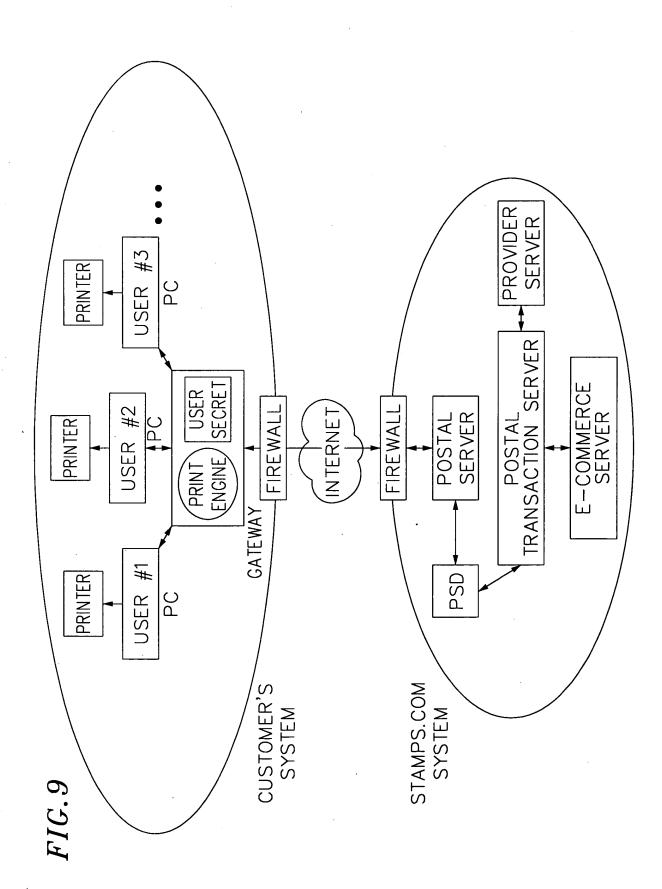
FIG. 7



ļ. A

6.18 8.18 8.18 B. B. B.





The first state state of the st

Į,ſŢ

FIG. 10

